P24609.P06

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Ming-Fong YEH et al.

Appln No. : 10/720,214 Group Art Unit: Unknown

Filed : Nov 25, 2003 Examiner: Unknown

For : DATA ENCRYPTION AND DECRYPTION METHOD AND APPARATUS

SUPPLEMENTAL CLAIM OF PRIORITY
SUBMITTING CERTIFIED COPY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Further to the Claim of Priority filed November 25, 2003 and as required by 37 C.F.R. 1.55, Applicant hereby submits a certified copy of the application upon which the right of priority is granted pursuant to 35 U.S.C. §119, i.e., of Chinese Application No.02 1 52606. 0, filed November 26, 2002.

Respectfully submitted,
Ming-fong YEH et al.

Bruce H. Bernstein
Reg. No. 29,027

January 7, 2004
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2002·11 26

申　请　号：　02 1 52606.0

申请类别：　发明

发明创造名称：　数据加密、解密方法及装置

申　请　人：　松下电器产业株式会社

发明人或设计人：叶明崳铮涣志裁担环骄

中华人民共和国
国家知识产权局局长　王景川

2003 年 11 月 19 日

权 利 要 求 书

1. 一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密算法模块指示符；

步骤 B. 输入待加密的数字数据；

步骤 C. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义数据取出；

步骤 D. 自取出的加密定义数据中，随机选取出一加密算法模块指示符；

步骤 E. 由上述所选取的加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理；及

步骤 F. 对经加密处理後的数字数据附加解密信息後予以输出的。

2. 按权利要求 1 所述的方法，其特征在于步骤 A 所建立的安全等级数据库中的加密定义字段包含有多个加密算法模块指示符及其对应采用比例；且步骤 D 自取出的加密定义数据中，依各个加密算法模块指示符及其对应采用比例配合乱数产生器及 MOD 运算选取出一加密算法模块指示符者。

3. 按权利要求 1 所述的方法，其特征在于步骤 A 所建立的安全等级数据库中的加密定义字段包含有多个加密算法模块组合，每个加密算法模块组合含有加密算法模块指示符及验证算法模块指示符；且步骤 D 自取出的加密定义数据中，随机选取出一加密算法模块组合；及步骤 E 由上述所选取的加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

4. 按权利要求 3 所述的方法，其特征在于步骤 A 所建立的安全等级数据库中的加密定义字段包含有多个加密算法模块组合及其对应采用比例；且步骤 D 自取出的加密定义数据中，依各个加密算法模块组合及其对应采用比例配合乱数产生器及 MOD 运算选取出一加密算法模块组合者。

5. 一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤 B. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密模块数据库索引；

步骤 C. 输入待加密的数字数据；

步骤 D. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义数据取出；

步骤 E. 自取出的加密定义数据中，随机选取出一加密模块数据库索引；

步骤 F. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 G. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；及

步骤 H. 对经加密处理後的数字数据附加解密信息後予以输出的。

6. 按权利要求 5 所述的方法，其特征在于步骤 B 所建立的安全等级数据库中的加密定义字段包含有多个加密模块数据库索引及其对应采用比例；且步骤 E 自取出的加密定义数据中，依各个加密模块数据库索引及其对应采用比例配合乱数产生器及 MOD 运算一加密模块数据库索引者。

7. 一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立一包含有多个加密算法模块指示符的加密定义数据；

步骤 B. 输入待加密的数字数据；

步骤 C. 从上述的加密定义数据，随机选取出一加密算法模块指示符；

步骤 D. 由上述所选取的加密算法模块指示符作指引，控制对输入数字数据做加密的加密处理；及

步骤 E. 对经加密处理後的数字数据附加解密信息後予以输出的。

8. 按权利要求 7 所述的方法，其特征在于步骤 A 所建立的加密定义数据包含有多个加密算法模块指示符及其对应采用比例；且步骤 C 依加密

定义数据中各个加密算法模块指示符及其对应采用比例配合乱数产生器及MOD运算选取出一加密算法模块指示符者。

9. 按权利要求7所述的方法，其特征在于步骤A所建立的加密定义数据包含有多个加密算法模块组合，每个加密算法模块组合含有加密算法模块指示符及验证算法模块指示符；且步骤C自取出的加密定义数据中，随机选取出一加密算法模块组合；及步骤D由上述所选取的加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

10. 按权利要求9所述的方法，其特征在于步骤A所建立的加密定义数据包含有多个加密算法模块组合及其对应采用比例；且步骤C自取出的加密定义数据中，依各个加密算法模块组合及其对应采用比例配合乱数产生器及MOD运算选取出一加密算法模块组合者。

11. 一种数据加密的方法，该方法包含下列步骤：

步骤A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤B. 建立一包含有多个加密模块数据库索引的加密定义数据；

步骤C. 输入待加密的数字数据；

步骤D. 从上述的加密定义数据，随机选取出一加密模块数据库索引；

步骤E. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤F. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；及

步骤G. 对经加密处理後的数字数据附加解密信息後予以输出的。

12. 按权利要求11所述的方法，其特征在于步骤B所建立的加密定义数据包含有多个加密模块数据库索引及其对应采用比例；且步骤D依加密定义数据中各个加密模块数据库索引及其对应采用比例配合乱数产生器及MOD运算一加密模块数据库索引者。

13. 一种数据加密的方法，该方法包含下列步骤：

步骤A. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应加密定义字段的安全等级数据库，该加密定义数据字段是加

密算法模块指示符；

步骤 B. 输入待加密的数字数据；

步骤 C. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义字段的加密算法模块指示符取出；

步骤 D. 由上述所选取的加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理；

步骤 E. 对经加密处理後的数字数据附加解密信息後予以输出的。

14. 按权利要求 13 所述的方法，其特征在于步骤 A 所建立的安全等级数据库中的加密定义字段是加密算法模块组合，该加密算法模块组合含有加密算法模块指示符及验证算法模块指示符；且步骤 C 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义字段的加密算法模块组合数据取出；及步骤 D 由上述所选取的加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

15. 一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤 B. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应加密定义字段的安全等级数据库，该加密定义数据字段是加密模块数据库索引；

步骤 C. 输入待加密的数字数据；

步骤 D. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义字段的加密模块数据库索引取出；

步骤 E. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 F. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；

步骤 G. 对经加密处理後的数字数据附加解密信息後予以输出的。

16. 一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，其特征在于还包括：

储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密算法模块指示符；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述安全等级数据库作更新的参数处理部；

由上述安全等级数据库寻找数据属性描述与上述检查部所送来的数字数据属性相符者、将其对应的加密定义数据传给下述加密选择部的属性检查部；

从取出的加密定义数据中，随机选取出一加密算法模块指示符的加密选择部；及

根据上述加密选择部所选取的一加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

17. 按权利要求 16 所述的装置，其特征在于安全等级数据库中的加密定义字段包含有多个加密算法模块指示符及其对应采用比例；且上述加密选择部是由取出的加密定义数据中，依各个加密算法模块指示符及其对应采用比例配合乱数产生器及 MOD 运算选取出一加密算法模块指示符者。

18. 按权利要求 16 所述的装置，其特征在于安全等级数据库中的加密定义字段包含有多个加密算法模块组合，每个加密算法模块组合含有加密算法模块指示符及验证算法模块指示符；且上述加密选择部是由取出的加密定义数据中，随机选取出一加密算法模块组合；及上述加密处理部是根据上述加密选择部所选取的一加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

19. 按权利要求 18 所述的装置，其特征在于安全等级数据库中的加密定义字段包含有多个加密算法模块组合及其对应采用比例；且上述加密选择部是由取出的加密定义数据中，依各个加密算法模块组合及其对应采用比例配合乱数产生器及 MOD 运算选取出一加密算法模块组合者。

20. 按权利要求 16 所述的装置，其特征在于还包括：

储存多个记录数据项，每个记录项含有加密算法模块指示符、及验

证算法模块指示符的加密模块数据库；且

上述安全等级数据库的加密定义字段包含有多个加密模块数据库索引；

上述加密选择部是由取出的加密定义数据中，随机选取出一加密模块数据库索引，再依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；及

上述加密处理部是根据上述加密选择部所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

21. 按权利要求 20 所述的装置，其特征在于安全等级数据库中的加密定义字段是包含有多个加密模块数据库索引及其对应采用比例；且上述加密选择部是由取出的加密定义数据中，依各个加密模块数据库索引及其对应采用比例配合乱数产生器及 MOD 运算取出一加密模块数据库索引，再依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项者。

22. 按权利要求 20 或 21 所述的装置，其参数处理部是由上述检查部所送来的参数数据对上述安全等级数据库及加密模块数据库作更新者。

23. 一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，其特征在于还包括：

储存多个记录数据项，每个记录项含有加密算法模块指示符的加密模块数据库；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述加密模块数据库作更新的参数处理部；

从上述加密模块数据库中，随机选取出记录项的加密选择部；及

根据上述加密选择部所选取的记录项做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

24. 按权利要求 23 所述的装置，其特征在于加密模块数据库是储存多个记录数据项，每个记录项包含有加密算法模块指示符及其对应采用比例；且上述加密选择部是依上述加密模块数据库中每个记录项所对应采用比例配合乱数产生器及 MOD 运算选取出记录项者。

25. 按权利要求 23 所述的装置，其特征在于加密模块数据库是储存多个记录数据项，每个记录项包含有加密算法模块指示符及验证算法模块指示符；且上述加密处理部是根据上述加密选择部随机所选取的记录项加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

26. 按权利要求 25 所述的装置，其特征在于加密模块数据库是储存多个记录数据项，每个记录项包含有加密算法模块指示符、验证算法模块指示符及其对应采用比例；且上述加密选择部是依上述加密模块数据库中每个记录项所对应采用比例配合乱数产生器及 MOD 运算从上述加密模块数据库中选取出记录项者。

27. 一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，其特征在于还包括：

储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段是加密算法模块指示符；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述安全等级数据库作更新的参数处理部；

由上述安全等级数据库寻找数据属性描述与上述检查部所送来的数字数据属性相符者、将其对应的加密定义数据传给下述加密处理部的属性检查部；及

根据上述属性检查部所取出的一加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

28. 按权利要求 27 所述的装置，其特征在于安全等级数据库中的加密定义字段是加密算法模块组合，该加密算法模块组合含有加密算法模块指示符及验证算法模块指示符；且加密处理部是根据上述属性检查部所取出的一加密算法模块组合做指引，控制对输入数字数据做何种加密及何种验证等加密处理者。

29. 一种数据解密方法，该方法包含下列步骤：

步骤 A. 输入待解密的数字数据；

步骤 B. 检查上述的数字数据是否含有解密算法模块指示符，如果有、则取出该解密算法模块指示符，如果否、则设定解密数据等於输入数据後至步骤 D 作处理；

步骤 C. 依据取出解密算法模块指示符作指引，控制对上述输入数字数据做解密的解密处理；及

步骤 D. 输出经解密後的数字数据。

30. 按权利要求 29 所述的方法，其特征在于步骤 B 检查上述的数字数据是否含有解密算法模块组合，该解密算法模块组合是含有解密算法模块指示符及验证算法模块指示符，如果有、则取出该解密算法模块组合，如果否、则设定解密数据等於输入数据至步骤 D 作处理；且步骤 C 由上述所选取的解密算法模块组合做指引，控制对输入数字数据做何种解密及何种验证等解密处理者。

31. 一种数据解密方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项是解密算法模块指示符的解密模块数据库；

步骤 B. 输入待解密的数字数据；

步骤 C. 检查上述的数字数据是否含有解密模块数据库索引，如果有、则取出解密模块数据库索引，如果否、设定解密数据等於输入数据至步骤 F 作处理；

步骤 D. 依取出的解密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 E. 由上述所选取的记录项做指引，控制对输入数字数据做解密的解密处理；及

步骤 F. 输出经解密後的数字数据。

32. 按权利要求 31 所述的方法，其特征在于步骤 A 建立储存多个记录数据项，每个记录项含有解密算法模块指示符及验证算法模块指示符的解密模块数据库；且步骤 E 由上述所选取的记录项做做指引，控制对输入数字数据做何种解密及何种验证等解密处理者。

33. 一种数据解密装置，该装置是备有输入数据的输入部及将解密

处理後数据予以输出的输出部，其特征在于还包括：

检查上述输入部输入的数据是否含有解密算法模块指示符，如果有、则取出该解密算法模块指示符，如果否、则直接将输入的数据传给输出部的检查部；及

根据上述检查部所取出的一解密算法模块指示符做指引，控制对输入数字数据做解密的解密处理的解密处理部者。

34. 按权利要求 33 所述的装置，其特征在于上述检查部是检查上述输入部输入的数据是否含有解密算法模块组合，该解密算法模块组合是含有解密算法模块指示符及验证算法模块指示符，如果有、则取出该解密算法模块组合，如果否、则直接将输入的数据传给输出部；且上述解密处理部是根据上述检查部所取出的一解密算法模块指示符做指引，控制对输入数字数据做何种解密及何种验证等解密处理者。

35. 按权利要求 33 所述的装置，其特征在于还包括：储存多个记录数据项，每个记录项含有解密算法模块指示符的解密模块数据库；且上述检查部是检查上述输入部输入的数据是否含有解密模块数据库索引，如果有、则取出该解密模块数据库索引并以此索引自解密模块数据库取出记录项，如果否、则直接将输入的数据传给输出部；及上述解密处理部是根据上述检查部所取出的记录项做指引，控制对输入数字数据做解密的解密处理者。

36. 按权利要求 35 所述的装置，其特征在于上述解密模块数据库是储存多个记录数据项，每个记录项含有解密算法模块指示符及验证算法模块指示符；且上述解密处理部是根据上述检查部所取出的记录项做指引，控制对输入数字数据做何种解密及何种验证等解密处理者。

37. 按权利要求 35 所述的装置，其特征在于还包括：以参数数据对上述解密模块数据库作更新的参数处理部；且上述检查部是检查并分离上述输入部输入的数据是为参数数据或数字数据，如为参数数据、则传给上述参数处理部，如为数字数据、则检查该数字数据是否含有解密模块数据库索引，如果有、则取出解密模块数据库索引并以此索引自解密模块数据库取出记录项，如果否、则直接将输入的数据传给输出部者。

38. 按权利要求 37 所述的装置，其特征在于上述解密模块数据库是储存多个记录数据项，每个记录项含有解密算法模块指示符及验证算法模块指示符；且上述解密处理部是根据上述检查部所取出的记录项做指引，控制对输入数字数据做何种解密及何种验证等解密处理者。

说　　明　　书

数据加密、解密方法及装置

技术领域

本发明涉及数据加密和解密方法及装置，其中，数据的加密和解密用数据属性匹配来集成，并在数据加密中经过动态选择机制交替使用不同加密算法模块组合，以达到对数据提供足够的安全性保护并兼顾处理速度。

背景技术

随着互联网的盛行，现在的企业都使用互联网来连接各地的分公司。为了保护企业在网路上传递的机密数据不被骇客窃取和篡改，都是以加密算法配合密钥(key)把数据进行加密的处理，使骇客无法知道数据的内容，以保护数据在网路上能安全的传递。并且利用杂凑函数(Hash function)进行数据的验证，确保数据不会遭到篡改。到现在已经有多家厂商的产品如思科(CISCO)公司的路由器，利用 RFC2401 的"互联网通讯安全协定"的技术来保护数据能在网路上安全传递。

加密算法是把数据转换成人类看不懂的形式，收到数据的人必须把数据解密的后才能知道数据本身的意义。经过加密的数据就算是在传输过程中被拦截，如果不知道如何解密，收到的数据如同垃圾一样。常见的加密算法有 DES、RSA、3DES、FEAL、IDEA 等等。

验证算法是把数据转换成固定长度的数值，而且无法从这个数值经由逆运算求得原来的数据。验证算法主要是用来确认通讯双方的身份及检验数据本身的完整性。例如把数据本身传给杂凑算法处理，可以得到一组校验和，然後连同数据一起传送出去，接收方可以利用校验和检查数据本身是否遭到窜改。常见的验证算法有 N-HASH、MD5、SHA1 等等。

数据分组是一种数据形式。在网路上传送或接收的数据都会被转换成数据分组的形式，传送数据的前先把数据切割成数据分组的格式，接收数据时再重新组合成原来的数据。数据分组在传送过程中发生错误时，接收

端只需要求错误的数据分组重新传送即可，可以有效节省传送时间。如果数据分组遭到窃取，只要没有得到全部的数据分组，亦无法得到完整的原始数据。

思科公司的路由器利用"互联网通讯安全协议"的技术作为保护数据在互联网上传递的安全。图 5 和图 6 示出了在此采用的数据加密及接密处理装置。在第 5 图中，50 是可输入明文数据的数据输入部。51 是根据使用者所决定的加密算法进行数据分组加密处理的加密部。52 是根据使用者所决定的验证算法进行数据分组验证处理的验证部。53 是将加密数据输出至存储器或其他储存装置的数据输出部。在第 6 图中，60 是可输入加密数据的数据输入部。61 是根据使用者所决定的验证算法进行数据分组验证处理的验证部。62 是根据使用者所决定的解密算法进行数据分组解密处理的解密部。63 是将明文数据输出至存储器或其他储存装置的数据输出部。

在数据加密装置端，从数据输入部 50 输入明文数据；的后在加密部 51 根据先前决定的加密算法和密钥，进行数据加密的处理；接着在验证部 52 根据先前决定的验证算法，进行验证数据的处理；最後将密文送到数据输出部 53 输出供利用。

在数据解密装置端，从数据输入部 60 输入加密数据；的后在验证部 61 根据先前决定的验证算法，进行验证数据的处理；接着解密部 62 根据先前决定的解密算法和密钥，进行解密数据的处理；最後明文数据由输出部 63 输出供利用。

上述用于互联网数据通讯安全传送及接收数据的处理装置，是利用加密算法和验证算法保证数据的安全性和正确性。如果考虑到数据的安全性和正确性而选用 3DES 算法来进行加密处理，SHA1 算法来进行验证处理，则会造成处理速度的降低；但是，为加快速度而仅选用 DES 算法来进行加密处理，MD5 算法来进行验证处理，则又会使数据的安全性和正确性大大的降低。所以，如何在安全性与加快处理速度取得一平衡点则将是一个重要的课题。

发明内容

为解决上述问题，本发明数据加密方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密算法模块指示符；

步骤 B. 输入待加密的数字数据；

步骤 C. 从上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义数据取出；

步骤 D. 从取出的加密定义数据中，随机选取出加密算法模块指示符；

步骤 E. 由上述所选取的加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理；及

步骤 F. 对经加密处理后的数字数据附加解密信息后予以输出。

本发明的另一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤 B. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密模块数据库索引；

步骤 C. 输入待加密的数字数据；

步骤 D. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义数据取出；

步骤 E. 自取出的加密定义数据中，随机选取出一加密模块数据库索引；

步骤 F. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 G. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；及

步骤 H. 对经加密处理後的数字数据附加解密信息後予以输出。

本发明的另一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立一包含有多个加密算法模块指示符的加密定义数据；

步骤 B. 输入待加密的数字数据；

步骤 C. 从上述的加密定义数据，随机选取出一加密算法模块指示符；

步骤 D. 由上述所选取的加密算法模块指示符作指引，控制对输入数字数据做加密的加密处理；及

步骤 E. 对经加密处理後的数字数据附加解密信息後予以输出。

本发明的另一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤 B. 建立包含有多个加密模块数据库索引的加密定义数据；

步骤 C. 输入待加密的数字数据；

步骤 D. 从上述的加密定义数据，随机选取出加密模块数据库索引；

步骤 E. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 F. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；及

步骤 G. 对经加密处理後的数字数据附加解密信息後予以输出。

本发明的另一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应加密定义字段的安全等级数据库，该加密定义数据字段是加密算法模块指示符；

步骤 B. 输入待加密的数字数据；

步骤 C. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义字段的加密算法模块指示符取出；

步骤 D. 由上述所选取的加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理；

步骤 E. 对经加密处理後的数字数据附加解密信息後予以输出。

本发明的另一种数据加密的方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项含有加密算法模块指示符及验证算法模块指示符的加密模块数据库；

步骤 B. 建立储存多个记录数据项，每个记录项含有数据属性描述字段及其对应加密定义字段的安全等级数据库，该加密定义数据字段是加密模块数据库索引；

步骤 C. 输入待加密的数字数据；

步骤 D. 由上述安全等级数据库寻找数据属性描述与上述数字数据属性相符者、将其对应的加密定义字段的加密模块数据库索引取出；

步骤 E. 依取出的加密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 F. 由上述所选取的记录项做指引，控制对输入数字数据做何种加密及何种验证等加密处理；

步骤 G. 对经加密处理後的数字数据附加解密信息後予以输出。

本发明的一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，装置还包括：

储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段包含有多个加密算法模块指示符；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述安全等级数据库作更新的参数处理部；

由上述安全等级数据库寻找数据属性描述与上述检查部所送来的数字数据属性相符者、将其对应的加密定义数据传给下述加密选择部的属性检查部；

从取出的加密定义数据中，随机选取出一加密算法模块指示符的加密选择部；及

根据上述加密选择部所选取的一加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

本发明的另一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，装置还包括：

储存多个记录数据项，每个记录项含有加密算法模块指示符的加密模块数据库；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述加密模块数据库作更新的参数处理部；

从上述加密模块数据库中，随机选取出记录项的加密选择部；及

根据上述加密选择部所选取的记录项做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

本发明的另一种数据加密装置，该装置是备有输入数据的输入部及将加密处理後数据予以输出的输出部，装置还包括：

储存多个记录数据项，每个记录项含有数据属性描述字段及其对应的加密定义字段的安全等级数据库，该加密定义字段是加密算法模块指示符；

检查并分离上述输入部输入的数据是为参数数据或数字数据的检查部；

由上述检查部所送来的参数数据对上述安全等级数据库作更新的参数处理部；

由上述安全等级数据库寻找数据属性描述与上述检查部所送来的数字数据属性相符者、将其对应的加密定义数据传给下述加密处理部的属性检查部；及

根据上述属性检查部所取出的一加密算法模块指示符做指引，控制对输入数字数据做加密的加密处理的加密处理部者。

本发明的一种数据解密方法，该方法包含下列步骤：

步骤 A. 输入待解密的数字数据；

步骤 B. 检查上述的数字数据是否含有解密算法模块指示符，如果有、则取出该解密算法模块指示符，如果否、则设定解密数据等於输入数据後至步骤 D 作处理；

步骤 C. 依据取出解密算法模块指示符作指引，控制对上述输入数字数据做解密的解密处理；及

步骤 D. 输出经解密後的数字数据。

本发明的另一种数据解密方法，该方法包含下列步骤：

步骤 A. 建立储存多个记录数据项，每个记录项是解密算法模块指示符的解密模块数据库；

步骤 B. 输入待解密的数字数据；

步骤 C. 检查上述的数字数据是否含有解密模块数据库索引，如果有、则取出解密模块数据库索引，如果否、设定解密数据等於输入数据至步骤 F 作处理；

步骤 D. 依取出的解密模块数据库索引，自上述加密模块数据库中选取记录项；

步骤 E. 由上述所选取的记录项做指引，控制对输入数字数据做解密的解密处理；及

步骤 F. 输出经解密後的数字数据。

本发明的一种数据解密装置，该装置是备有输入数据的输入部及将解密处理後数据予以输出的输出部，装置还包括：

检查上述输入部输入的数据是否含有解密算法模块指示符，如果有、则取出该解密算法模块指示符，如果否、则直接将输入的数据传给输出部的检查部；及

根据上述检查部所取出的一解密算法模块指示符做指引，控制对输入数字数据做解密的解密处理的解密处理部者。

根据本发明的数据加密装置上述的构成，使用者由输入部输入数据，由检查部检查并分离所输入的数据为参数数据或待加密数据，如是参数数据、则交由参数处理部更新安全等级数据库或加密模块数据库；如为待加密数据、则交由属性检查部处理。属性检查部从安全等级数据库寻找数据属性描述与输入数据属性相符者，将其加密定义数据取出传给加密选择部。加密选择部由加密定义数据中动态选出一加密模块数据库索引，并以此由加密模块数据库取得一笔加密模块组合记录，并将其传给加密处理部。加密处理部依传来的加密模块组合控制对输入的待加密数据做何种加密及何种验证等加密处理。最後由输出部附加解密信息後输出。

本发明也提供使用者一种数据解密装置根据本发明的数据解密装置上述的构成，使用者由输入部输入数据，由检查部检查分离所输入的数据为参数数据或待解密的数字数据，如是参数数据、则交由参数处理部更新解密模块数据库；如为待解密数据则检查其是否含有解密信息，如果有、则由解密信息中取出解密模块数据料库索引，并以此从解密模块数据库取初一笔解密模块组合记录，并将其传给解密处理部处理；如果否、则将输入的数字数据传给输出部作输出。解密处理部依传来的解密模块组合控制对输入的待解密数据做何种解密及何种验证等解密处理。最後由输出部作输出。

附图说明

第 1 图 是本发明的数据加密装置的最佳实施例的方块图。

第 2 图 是本发明的数据解密装置的最佳实施例的方块图。

第 3 图 是本发明的数据加密装置的实施例中的数据加密动作流程图。

第 4 图 是本发明的数据解密装置的实施例中的数据解密动作流程图。

第 5 图 是习知例的数据加密装置的是统方块图。

第 6 图 是习知例的数据解密装置的是统方块图。

第 7 图 是本发明的数据加密装置的实施例中的安全等级数据库的结构示意图。

第 8 图 是本发明的数据加密装置的实施例中的安全等级数据库中数据属性描述数据可使用的数据属性描述指令说明表。

第 9 图 是本发明的数据加密装置的实施例中的安全等级数据库中加密定义数据的结构示意图。

第 10 图 是本发明的数据加密装置的实施例中的加密模块数据库的结构示意图。

第 11 图 是本发明的数据加密装置的实施例中的解密模块数据库的结构示意图。

第 12 图 是本发明的数据加密装置的实施例中的输入数据的结构示意图。

第 13 图 是本发明的数据加密装置的实施例中的输出数据的结构示意图。

第 14 图 是本发明的数据加密装置的实施例中的处理范例。

第 15 图 是本发明的数据解密装置的实施例中的处理范例。

第 16 图 是本发明的另一种数据加密装置的实施例的方块图。

第 17 图 是本发明的另一种数据加密装置的实施例的方块图。

具体实施方式

第 1 图是本发明的数据加密装置的最佳实施例的方块图。在第 1 图

中：

109 是安全等级数据库，储存着多个记录的数据项，每个记录项包含有数据属性描述及其对应的加密定义数据，其中数据属性描述占 24 个字节，加密定义数据占 8 个字节，其构造示意图如第 7 图所示。数据属性描述用於对输入数据分组数据作属性比对的用，乃是由逻辑运算子及条件运算式所构成，且其总长度不得超过 24 个字节，如不足 24 字节，则必须於属性描述数据结尾加上结束值 FF 作结束，有关数据属性描述指令其说明如第 8 图所示。加密定义数据用於动态选取加密算法模块之用，是由 4 组数据所构成，每组数据含的加密算法模块索引占 1 字节及其采用比例值占 1 字节所构成。加密定义数据如不足 4 组则必须於其结尾填上 FF，其结构示意图如图第 9 图所示。

111 是加密模块数据库，储存着对输入数据进行加密时的加密算法、验证算法及整体验证算法的各种组合的相关数据。加密模块数据库的构造示意图如第 10 图所示，一种组合由一个记录来表示，每个记录项包含有数据加密算法指示符、数据验证算法指示符及整体验证算法指示符，每个指示符亦即该算法程式的所在位址由 4 个字节组成。数据加密算法指示符，其内容可为：

DES 加密算法指示符，或

3DES 加密算法指示符，或

RSA 加密算法指示符，或

RC4 加密算法指示符，或

FEAL 加密算法指示符，或

IDEA 加密算法指示符，或

TWOFISH 加密算法指示符。

数据验证算法指示符及整体验证算法指示符，其内容可为：

MD5 验证算法指示符，或

SHA1 验证算法指示符，或

N-HASH 验证算法指示符。

本实施例以 7 种加密算法及 3 种验证算法而言，并考虑不加密及不验证的场合，加密模块数据库最多可有(7+1)*(3+1)*(3 +1)=128 个记录项。

110 是数据缓存区，为暂时储存加密选择部所产生的序列数据、参数检查部存入的加密模块验算法相关数据及数据属性检查部、加密控制部处理过程中所需的缓存数据。

100 是输入部，由键盘或其他任何可输入一般待加密数据或参数数据的输入器所构成。

101 是检查部，检查输入数据，若其为参数数据则交由参数处理部处理；否则传给属性检查部处理。

102 是属性检查部，由安全等级数据库 109 寻找数据属性描述字段所储存的数据属性与输入数据属性相符者，并将其对应的加密定义数据传给下述加密选择部取得加密模块数据库的索引，并将此索引连同输入数据传给加密控制部处理。

103 是加密选择部，依加密定义数据中各组加密模块数据库的索引及其采用比例值在数据缓存区 110 产生以各组采用比例值循序存放相对应数索引的序列，由乱数产生器产生一数值再以各组采用比例总和为分母作 MOD 运算得余数，以此余数为索引从的前产生序列取得加密模块数据库索引，并将结果及欲加密数据传加密处理部。

104 是加密控制部，依加密模块数据库索引取得数据加密算法指示符、数据验证算法指示符及整体验证算法指示符并依各指示符所指向的算法模块对输入数据作加密处理。

105 是加密部，根据加密算法指示符及其所需相关数据对输入数据作加密处理，并将结果传回加密控制部。

106 是验证部，根据验证算法指示符及其所需相关数据对输入数据作验证处理，并将结果传回加密控制部。

107 是输出部，将加密数据附加解密信息後输出至存储器或其他输出装置。

108 是参数处理部，核对检查部输入的参数数据，如果参数为加密算法模块参数、则更新至加密算法模块数据库；如为安全等级数据参数、则更新至安全等级数据库；如皆不是，则传回错误码。

第 3 图是本发明的数据加密装置的实施例中的数据加密动作流程图。於第 1 图的方块图中，当检查部 101 判断输入数据为欲加密数据时，即由

属性检查部 102 开始动作。第 3 图中，步骤 S301 储存输入的数据，然後进入属性检查部 102，找出该数据其属性所对应的加密定义数据，首先步骤 S302 读入一笔安全定义数据，接着步骤 S303 判断其数据属性描述字段是否为空白，如果是、则表示其为预设安全等级数据直接至步骤 S306；如果不是、则依数据属性描述字段数据一一检查输入数据内容，步骤 S304 判断数据属性是否相符，如果是至步骤 S306；如果不是、则重回步骤 S302。步骤 S306 即进入加密选择部 103 开始动态选取加密算法模块组合。首先，步骤 S306 判断加密定义数据是否只有一笔加密算法模块组合，如果是、则表示不须执行动态选取动作，至步骤 S307 设定使用此一模块组合，然後至步骤 S309；如果否至步骤 S308 依各模块采用比例，产生一序列，配合乱数产生器产生一数值再以各组采用比例总和为分母作 MOD 运算得余数，以此余数为索引依的前序列数据取得加密算法模块组合後接 S309。步骤 S309 即进入加密处理部 104 开始数据加密处理。首先，步骤 S309 依加密算法模块合数据取得各个模块指示符後，接下来步骤 S310 判断数据加密算法指示符是否为 0，如果为 0、则表示不执行加密处理，接步骤 S312；如果不为 0、则接步骤 S311 将此加密指示符及该指示符所需参数连同输入数据由加密部 105 处理加密後得到加密结果後接步骤 S312。步骤 S312 判断数据验证算法指示符是否为 0，如果为 0、则表示不执行数据验证处理，接步骤 S314；如果不为 0、则接步骤 S313 将此验证指示符及该指示符所需参数连同目前处理处理结果数据由验证部 106 处理验证後得到验证结果後接步骤 S314。步骤 S314 判断整体验证算法指示符是否为 0，如果为 0、则表示不执行整体验证处理，接步骤 S316；如果不为 0、则接步骤 S315 将此验证指示符及该指示符所需参数连同目前处理处理结果数据及首标数据由验证部 106 处理验证後得到验证结果後接步骤 S316。步骤 S316 将加密数据附加解密信息後输出至存储器或其他装置。

第 12 图是本发明数据加密装置的实施例中的输入数据分组数据结构图。在第 12 图中，输入数据是为互联网通讯的 IP 数据分组由 IP 首标及传送数据所构成，其首标数据中，VERS 是表示 IP 数据分组使用版本，大小为 4bits； HLEN 是表示 IP 数据分组首标组成以 32 位元为单位的长度，大小为 4bits；SVERICE TYPE 是表示 IP 数据分组服务形态为何，大小为

8bits； TOTAL LENGTH 是表示 IP 数据分组总长度大小，大小为 16bits；IDENTIFICATION 是表示 IP 数据分组辨识数据，大小为 16bits；FLAGS 是表示 IP 数据分组旗标数据，大小为 4bits； FRAGMENT OFFSET 是表示 IP 数据分组的数据的位移位址，大小为 12bits；TIME TO LIVE 是表示 IP 数据分组於互联网传递最长时间，单位为秒，大小为 8bits；PROTOCOL 是表示 IP 数据分组数据字段的通讯协定值，大小为 8bits； HEADER CHECKSUM 是表示 IP 数据分组首标的 check sum 数据，大小 16bits；SOURCE IP ADDRESS 是表示 IP 数据分组来源 IP 位址大小为 32bits；DESTINATION IP ADDRESS 是表示 IP 数据分组目的 IP 位址大小为 32bits；IP OPTIONS 是 IP 数据分组首标额外数据，大小最多为 40bits；PADDING 是作为 IP 数据分组首标长度补至 4 字节倍数用。

第 13 图是本发明数据加密装置的实施例中的输出数据结构图。输出数据是为 IP 首标、解密信息数据及加密数据所构成。

接着说明本发明数据加密装置的实施例的处理范例。第 14 图是本发明数据加密装置的实施例的处理范例的数据。在第 14 图中： 14b 是本处理范例於加密动作流程刚开始的安全等级数据库的数据。14c 是本处理范例於加密动作流程刚开始的加密模块数据库的数据。14a 是本处理范例於加密动作流程刚开始的输入数据。在第 3 图中，步骤 S301 接受输入数据(如图 14a)後，步骤 S302 从安全等级数据库数据中(如图 14b)读入第一笔数据，其数据属性描述数据前 14 字节为"01 04 18 C0A80000 05 18 AC100000 FF"，後 10 字节皆为"FF"，加密定义数据为"01 03 02 03 03 01 04 01"，步骤 S303 判断数据属性描述数据不是空白，直接至步骤 S304。步骤 S304 首先依第 8 图数据属性描述指令说明表，将数据属性描述数据编译为当输入数据分组数据中的来源 IP 位址与 C0A80000 两者前 24bit 值为相同且目的 IP 位址与 AC100000 两者前 24bit 值为相同者时，则为真；否则为假。接着从输入数据(如图 14a)内容可知来源 IP 位址 C0A80001 与 C0A80000 两者前 24bit 值为相同；且目的 IP 位址 AC100001 与 AC100000 两者前 24bit 值为相同故设定数据属性为相符。步骤 S305 依步骤 S304 所得结果为数据属性相符直接至步骤 S306。步骤 S306 检查加密定义数据是否只有一笔数据，由於其为 01 03 02 03 03 01 04 01，是不只一笔加

密算法模块组合故至步骤 S308。步骤 S308 依目前加密定义数据中加密模块数据库索引及其采用比例产生 3 个 01、3 个 02、1 个 03 及 1 个 04 的连续序列 01 01 01 02 02 02 03 04，其总长度为各采用比例总和 8，以乱数器产生一数值为 5318659，将此数作 MOD 8 运算得 3，其对应至序列值为 02，故所选择的加密模块数据库索引为 02，接着至步骤 S309。步骤 S309 依加密模块数据库索引值 02 从加密模块数据库数据(如图 14c)中取得其加密算法模块分别为数据加密算法指示符为 DES 加密算法指示符、数据验证算法指示符为 SHA1 验证算法指示符及整体验证算法指示符为 MD5 验证算法指示符，接着至步骤 S310。步骤 S310 依数据加密算法指示符为 DES 加密算法指示符不为 0，接着至步骤 S311。步骤 S311 将 DES 加密算法指示符及输入数据(如图 14a)的数据字段数据传给加密部作加密处理，接着至步骤 S312。步骤 S312 依数据验证算法指示符为 SHA1 验证算法指示符不为 0，接着至步骤 S313。步骤 S313 将 SHA1 验证算法指示符及步骤 S311 加密处理的结果传给验证部作数据验证处理，接着至步骤 S314。步骤 S314 依整体验证算法指示符为 MD5 验证算法指示符不为 0，接着至步骤 S315。步骤 S315 将 MD5 验证算法指示符、输入数据(如图 14a)的首标字段数据及步骤 S313 数据验证处理的结果传给验证部作整体验证处理，接着至步骤 S316。步骤 S316 将步骤 S315 处理所得结果加上解密信息标签及解密模块数据库索引值 02 後完成输出数据(如图 14a)後输出至其他装置。第 14 图中，14d 是本处理范例於加密动作流程结束的输出数据，其中解密信息数据为解密信息标签及解密模块数据库索引值为 2。

第 16 图是本发明的另一种数据加密装置的实施例的方块图。第 16 图中，并不须第 1 图中的安全等级数据库 109 及属性检查部 102。且 108 是参数处理部，检查检查部输入的参数数据，如果参数旗标字段是加密算法模块参数旗标、则依其数据字段中的加密算法模块辨识码，将加密算法模块参数存至数据缓存区 110 该加密算法模块对应的参数数据存放位址；且加密选择部 102 则直接使用存於数据缓存区的加密定义数据来动态选取加密算法模块组合。

又第 17 图是本发明的另一种数据加密装置的实施例的方块图。第 17 图中，并不须如第 1 图中的加密选择部 103；安全等级数据库 109 的加密

定义数据只存一加密算法模块组合数据；且属性检查部 102 直接将符合输入数据属性描述数据所对应的加密定义数据所存加密算法模块组合数据及连同输入传给加密处理部 104 处理。

第 2 图是本发明的数据解密装置的最佳实施例的方块图。在第 2 图中：

208 是解密模块数据库，储存着对输入数据进行解密时的解密算法、验证算法及整体验证算法的各种组合的相关数据。解密模块数据库，其构造示意图如第 11 图所示，一种组合由一个记录来表示，每个记录项包含有数据解密算法指示符、数据验证算法指示符及整体验证算法指示符，每个指示符亦即该算法程式的所在位址由 4 个字节组成。数据解密算法指示符，其内容可为：

DES 解密算法指示符，或

3DES 解密算法指示符，或

RSA 解密算法指示符，或

RC4 解密算法指示符，或

FEAL 解密算法指示符，或

IDEA 解密算法指示符，或

TWOFISH 解密算法指示符。

数据验证算法指示符及整体验证算法指示符，其内容可为：

MD5 验证算法指示符，或

SHA1 验证算法指示符，或

N-HASH 验证算法指示符。

本实施例以 7 种解密算法及 3 种验证算法而言，并考虑不解密及不验证的场合，解密模块数据库至多可有(7+1)*(3+1)*(3 +1)=128 笔记录。

207 是数据缓存区，为暂时储存参数处理部存入的解密验证相关数据及数据检查部、解密验证控制部处理过程中所需的缓存数据。

200 是输入部，由键盘或其他任何可输入数据数据分组的装置所构成。

201 是检查部，检查输入数据为参数数据则交由参数处理部处理；否则检查是否有解密信息标签，如果否、则传回错误码；如果有、则将输入数据分解出解密模块数据库索引及加密数据，并将其传给解密处理部处理。

202 是解密控制部，依解密模块数据库索引取得数据解密算法指示符、数

据验证算法指示符及整体验证算法指示符并依各指示符所指向的算法模块对输入数据作解密处理。

203 是验证部根据验证算法指示符及其所需相关数据对输入数据作验证处理，并将结果传回解密控制部。

204 是解密部根据解密算法指示符及其所需相关数据对输入数据作解密处理，并将结果传回解密控制部。

205 是输出部将解密数据输出至存储器或其他输出装置。

206 是参数处理部，检查由检查部输入的参数数据，如果为加密算法模块数据、则更新至加密算法模块数据库；如果否、则传回错误码。

第 4 图是本发明数据解密装置的实施例中的数据解密动作流程图。於第 2 图的方块图中，当检查部 201 判断输入数据为欲解密数据时于步骤 S401 接收数据输入，步骤 S402 判断其是否含有解密信息标签，如果没有、则表示输入数据有误，接步骤 S404 传回错误码後结束；如果有、则接步骤 S403 将输入数据分解出解密算法模块组合数据及加密数据。接着步骤 S405 判断解出解密算法模块组合数据是否正确，如果不正确、则接步骤 S407 传回错误码後结束；如果为正确、则接步骤 S406。步骤 S406 即进入解密控制部 202 开始数据解密处理。首先，步骤 S406 依解密算法模块组合数据取得各个解密算法模块指示符後，接下来步骤 S408 判断整体验证算法指示符是否为 0，如果为 0、则表示不执行整体验证处理，接步骤 S412；如果不为 0、则接步骤 S409 将此验证指示符及该指示符所需参数连同加密数据及首标数据由验证部 204 处理验证後得到验证结果後接步骤 S410 判断验证结果是否正确，如不正确、则至步骤 S411 传回错误码後结束；如果正确、则接步骤 S412。步骤 S412 判断数据验证算法指示符是否为 0，如果为 0、则表示不执行数据验证处理，接步骤 S416；如果不为 0、则接步骤 S413 将此验证指示符及该指示符所需参数连同加密数据由验证部 204 处理验证後得到验证结果後接步骤 S414 判断验证结果是否正确，如不正确、则至步骤 S415 传回错误码後结束；如果正确、则接步骤 S416。步骤 S416 判断数据加密算法指示符是否为 0，如果为 0、则表示不执行数据验证处理，接步骤 S420；如果不为 0、则接步骤 S417 将此验证指示符及该指示符所需参数连同加密数据由验证部 203 处理验证後得到验证结

果後接步驟 S418 判断验证结果是否正确，如不正确、则至步骤 S419 传回错误码後结束；如果正确、则接步骤 S420。步骤 S420 将解密数据输出至存储器或其他装置。

接着说明本发明数据解密装置的实施例的处理范例。第 15 图是本发明数据解密装置的实施例的处理范例的数据。在第 15 图中：15a 是本处理范例於解密动作流程刚开始的输入数据，其中含有解密信息标签及解密模块数据库索引值为 2 及加密数据。15b 是本处理范例於解密动作流程刚开始的解密模块数据库的数据。15c 是本处理范例於解密动作流程结束的输出数据。在第 4 图本发明数据解密装置的实施例中的数据解密动作流程图中，步骤 S401 接受输入数据(如图 15a)後，步骤 S402 判断含有解密信息标签後，步骤 S403 将输入数据如图 15a 分解出解密模块数据库索引值为 2 及加密数据。步骤 S405 判断解密模块数据库索引值是 2 为正确数据，直接至步骤 S406。步骤 S406 依解密模块数据库索引值 2 从解密模块数据库数据中(如图 15b)取得其解密算法模块分别为数据解密算法指示符为 DES 解密算法指示符、数据验证算法指示符为 SHA1 验证算法指示符及整体验证算法指示符为 MD5 验证算法指示符，接着至步骤 S408。步骤 S408 依整体验证算法指示符为 MD5 验证算法指示符不为 0，接着至步骤 S409。步骤 S409 将 MD5 验证算法指示符、输入数据(如图 15a)的首标字段数据及步骤 S403 分解出的加密数据传给验证部作整体验证处理，接着至步骤 S410。步骤 S410 判断整体验证结果为正确，接着至步骤 S412。步骤 S412 依数据验证算法指示符为 SHA1 验证算法指示符不为 0，接着至步骤 S413。步骤 S413 将 SHA1 验证算法指示符及步骤 S403 分解出的加密数据传给验证部作数据验证处理，接着至步骤 S414。步骤 S414 判断数据验证结果为正确，接着至步骤 S416。步骤 S416 依数据解密算法指示符为 DES 解密算法指示符不为 0，接着至步骤 S417。步骤 S417 将 DES 解密算法指示符及步骤 S403 分解出的加密数据传给解密部作解密处理，接着至步骤 S418。步骤 S418 判断数据解密结果为正确，接着至步骤 S420。步骤 S420 依输入数据(如图 15a)及步骤 S418 所得解密结果完成输出数据(如图 15c)後输出至其他装置。

本发明不限於上述的实施例，只要不改变其要旨而予以适当的变形皆

可实施，例如处理的输入数据不限定於数据分组数据，亦可为非数据分组型式的数字数据。又例如本发明的安全等级数据库的加密定义数据只存加密模块数据库索引及其采用比例；也可以同时储存加密算法指示符、数据验证算法指示符、整体验证算法指示符以及其采用比例而不须将加密算法模块组合数据另存於加密模块数据库中。又本发明的实施例虽以处理数据分组数据为例，其他形式的数据亦可比照实施。

依上述的说明，本发明的数据加密装置可以解决以往例的问题点，换言的，其效果是：可以根据数据属性的不同，自动切换加密算法模块组合，例如当使用者阅读其远端主机信件时，其认证其间的传输数据应受到最安全的加密算法模块组合来加密处理，而其他传输数据则采用交叉不同加密算法模块组合，如此，使用者登入帐户及加密不至外流，及其他传输数据经由交叉不同加密算法模块组合加密处理，不是合法者要窥探其内容更是困难；同时，其对传输时间的需求，可藉由调整各个加密算法模块组合使用比例来改善。

说 明 书 附 图

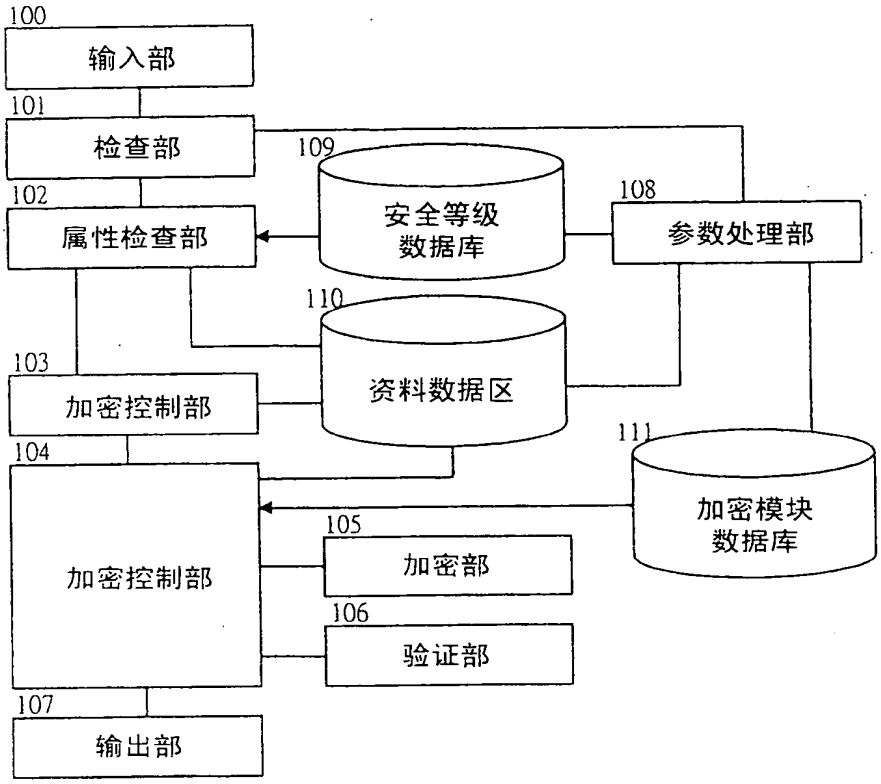

100
输入部
101
检查部
102
属性检查部
103
加密控制部
104
加密控制部
105
加密部
106
验证部
107
输出部
109
安全等级
数据库
108
参数处理部
110
资料数据区
111
加密模块
数据库

图 1

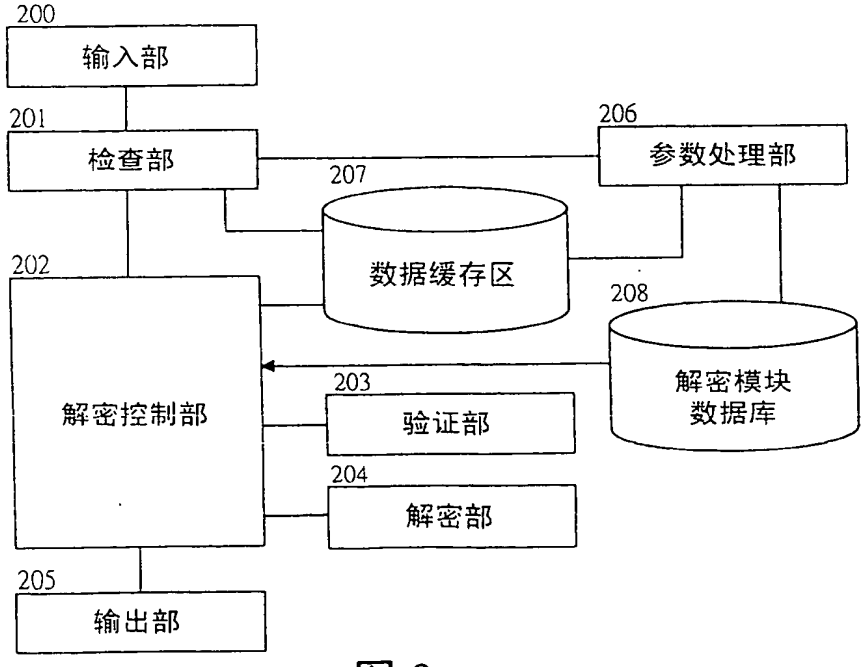

200
输入部
201
检查部
202
解密控制部
203
验证部
204
解密部
205
输出部
206
参数处理部
207
数据缓存区
208
解密模块
数据库

图 2

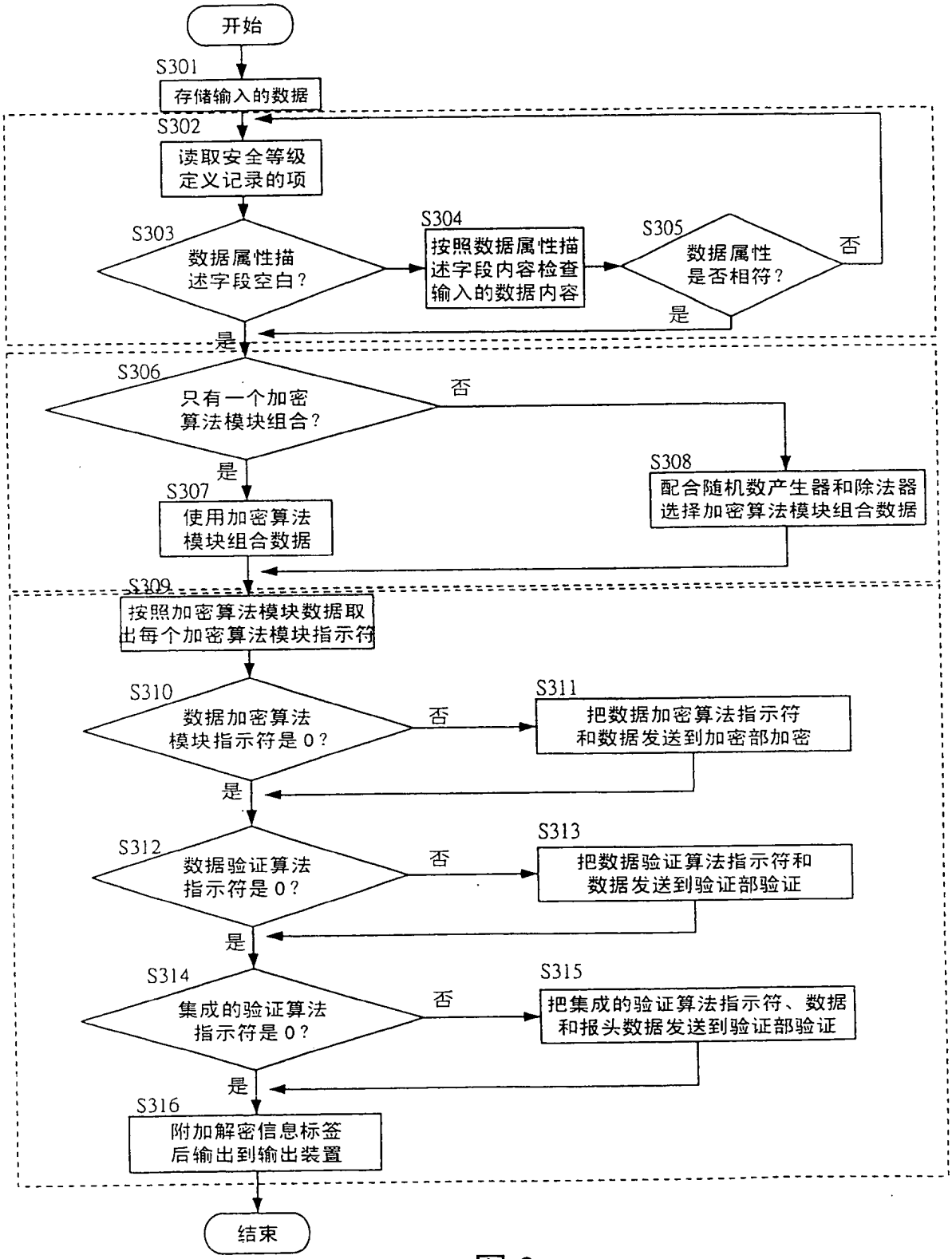

开始
S301
存储输入的数据
S302
读取安全等级
定义记录的项
S303
数据属性描
述字段空白？
S304
按照数据属性描
述字段内容检查
输入的数据内容
S305
数据属性
是否相符？
否
是
是
S306
只有一个加密
算法模块组合？
否
是
S307
使用加密算法
模块组合数据
S308
配合随机数产生器和除法器
选择加密算法模块组合数据
S309
按照加密算法模块数据取
出每个加密算法模块指示符
S310
数据加密算法
模块指示符是0？
否
S311
把数据加密算法指示符
和数据发送到加密部加密
是
S312
数据验证算法
指示符是0？
否
S313
把数据验证算法指示符和
数据发送到验证部验证
是
S314
集成的验证算法
指示符是0？
否
S315
把集成的验证算法指示符、数据
和报头数据发送到验证部验证
是
S316
附加解密信息标签
后输出到输出装置
结束

图 3

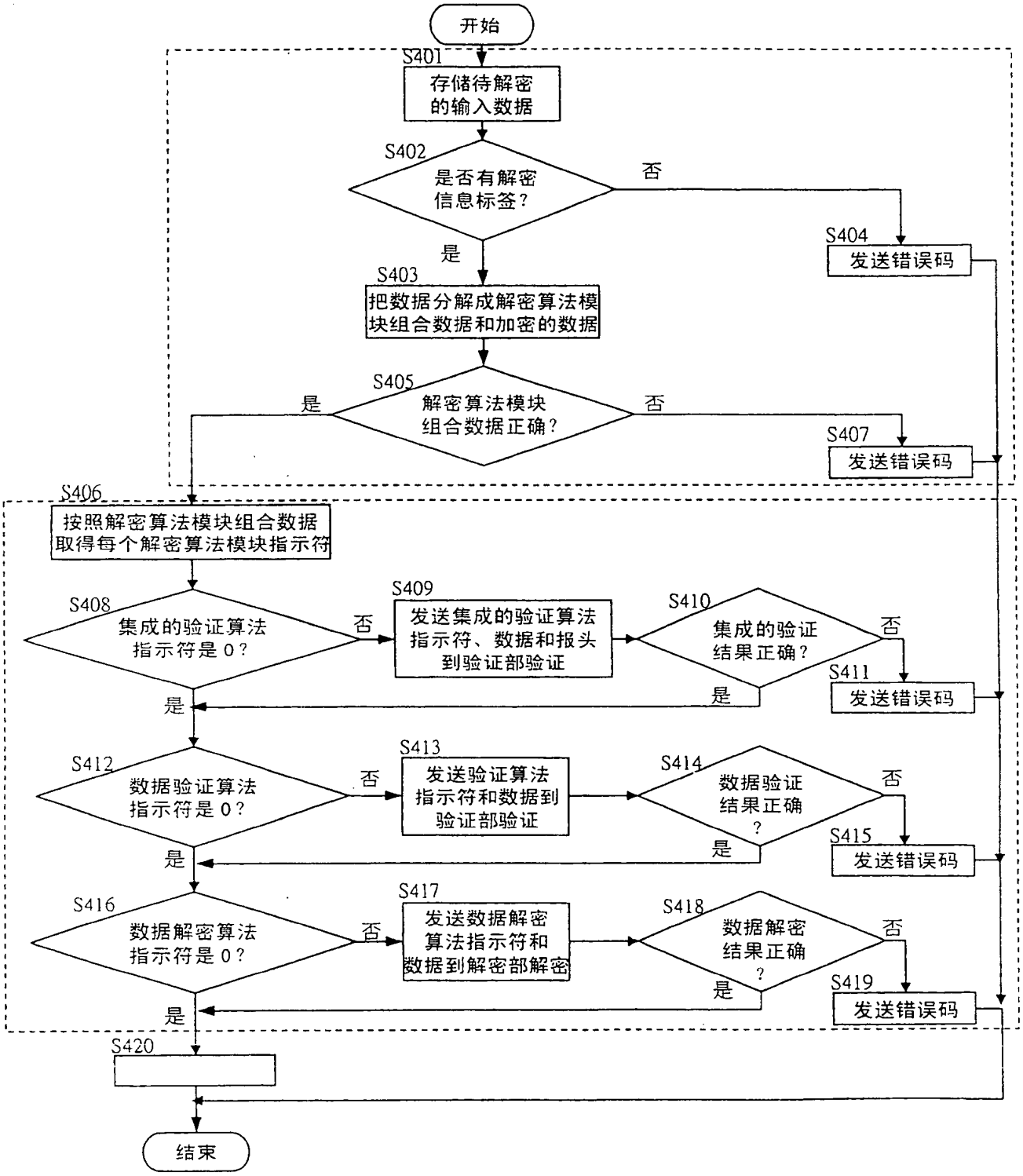

开始
S401
存储待解密的输入数据
S402
是否有解密信息标签？
否
是
S404
发送错误码
S403
把数据分解成解密算法模块组合数据和加密的数据
S405
解密算法模块组合数据正确？
是
否
S407
发送错误码
S406
按照解密算法模块组合数据取得每个解密算法模块指示符
S408
集成的验证算法指示符是0？
否
是
S409
发送集成的验证算法指示符、数据和报头到验证部验证
S410
集成的验证结果正确？
否
是
S411
发送错误码
S412
数据验证算法指示符是0？
否
是
S413
发送验证算法指示符和数据到验证部验证
S414
数据验证结果正确？
否
是
S415
发送错误码
S416
数据解密算法指示符是0？
否
是
S417
发送数据解密算法指示符和数据到解密部解密
S418
数据解密结果正确？
否
是
S419
发送错误码
S420
结束

图 4

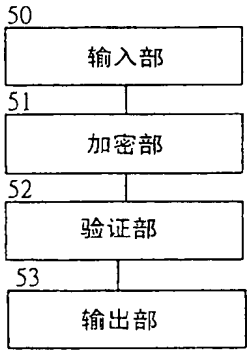


图 5

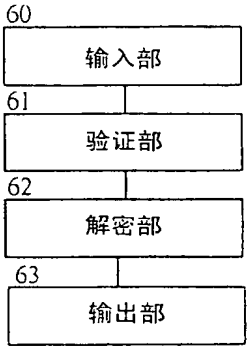


图 6

数据属性描述 （24字节）	加密定义字段 （8字节）
数据属性描述 1	加密定义 1
数据属性描述 2	加密定义 2
数据属性描述 3	加密定义 3
资料属性描述 N	加密定义 N

图 7

数据属性描述指令	说明
00	空白数据属性描述值，表明预设的安全等级定义记录
逻辑运算子	
01 expr1 expr2	AND运算子 expr1 AND expr2
02 expr1 expr2	OR运算子 expr1 OR expr2
03 expr1	NOT运算子NOT expr1
条件运算子	
04 AA BBBBBBBB	源地址 IP与 BBBBBBBB前 AA个字节相同
05 AA BBBBBBBB	目的地址 IP与 BBBBBBBB前 AA个字节相同
06 AA	通讯协议值为 AA
07 AAAA BB	数据地址 AAAA一字节值与 BB相同
08 AAAA BBBB	数据地址 AAAA二字节值与 BBBB相同
09 AAAA BBBBBBBB	数据地址 AAAA四字节值与 BBBBBBBB相同
0A～FE	保留值
FF	数据属性描述字段结束值

图 8

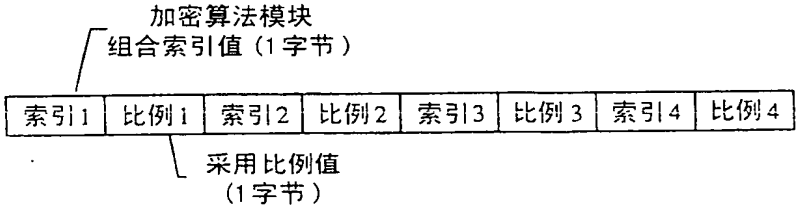


图 9

索引	数据加密算法指示符字段（4字节）	数据验证演算法指示符字段（4字节）	集成验证演算法指示符字段（4字节）
1	数据加密算法指示符1	数据验证算法指示符1	整体验证算法指示符1
2	数据加密算法指示符2	数据验证算法指示符2	整体验证算法指示符2
3	数据加密算法指示符3	数据验证算法指示符3	整体验证算法指示符3
N	数据加密算法指示符N	数据验证算法指示符N	整体验证算法指示符N

图 10

索引	数据加密算法指示符字段（4字节）	数据验证演算法指示符字段（4字节）	集成验证算法指示符字段（4字节）
1	数据解密算法指示符1	数据验证算法指示符1	整体验证算法指示符1
2	数据解密算法指示符2	数据验证算法指示符2	整体验证算法指示符2
3	数据解密算法指示符3	数据验证算法指示符3	整体验证算法指示符3
N	数据解密算法指示符N	数据验证算法指示符N	整体验证算法指示符N

图 11

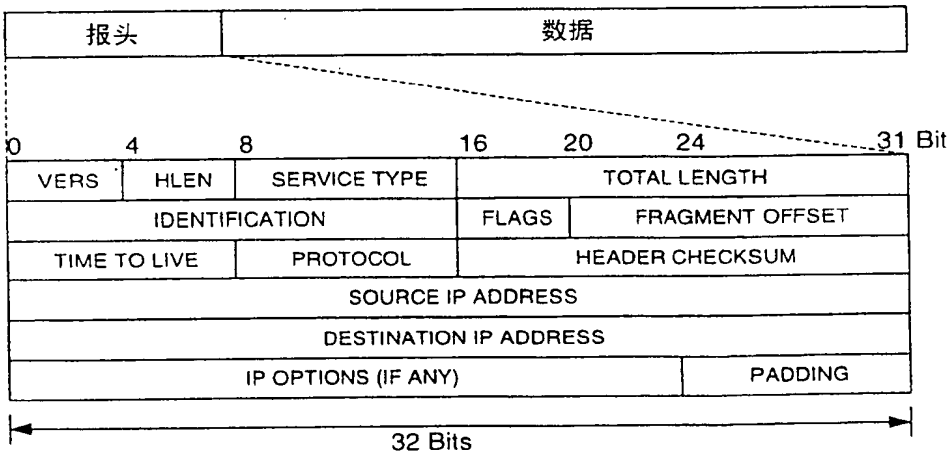


图 12

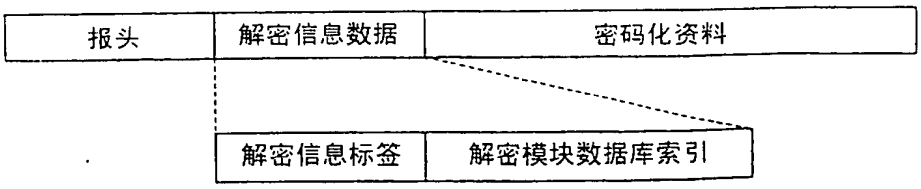
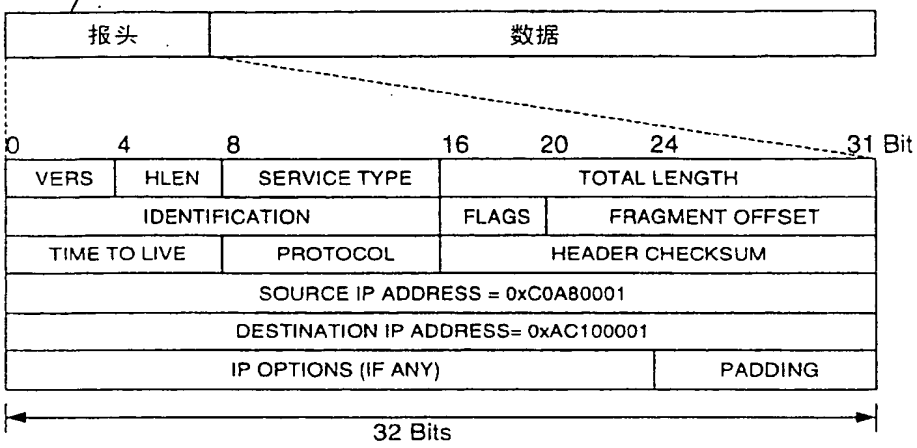


图 13

14a



14b

数据属性描述字段	加密定义字段
01 04 18 C0A80000 05 18 AC100000 FF ...	01 03 02 03 03 01 04 01
02 09 0034 55534552 09 0034 50415353 FF ...	03 01 FF ...
07 00 09 50 FF ...	04 01 FF ...
01 07 00 09 51 07 00 14 50 FF ...	05 01 FF ...
00 FF ...	01 05 02 04 04 01 FF ...

14c

索引	数据加密算法指示符字段	数据验证算法指示符字段	整体验证算法指示符字段
1	DES 加密算法指示符	MD5 验证算法指示符	0
2	DES 加密算法指示符	SHA1验证算法指示符	MD5验证算法指示符
3	3DES加密算法指示符	SHA1验证算法指示符	SHA1验证算法指示符
4	0	0	SHA1验证算法指示符
5	0	0	0

14d

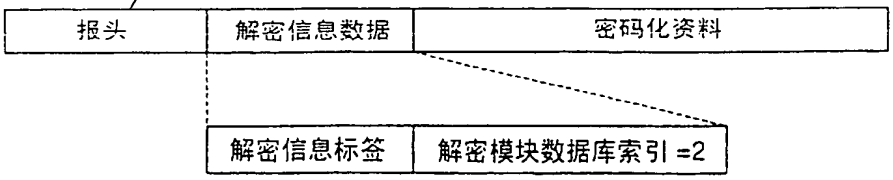
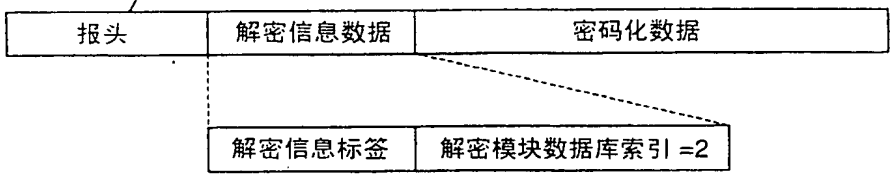


图 14

15a



15b

索引	数据解密算法指示符字段	数据验证算法指示符字段	整体验证算法指示符字段
1	DES 解密算法指示符	MD5 验证算法指示符	0
2	DES 解密算法指示符	SHA1 验证算法指示符	MD5 验证算法指示符
3	3DES 解密算法指示符	SHA1 验证算法指示符	SHA1验证算法指示符
4	0	0	SHA1验证算法指示符
5	0	0	0

15c

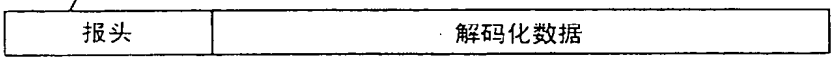


图 15

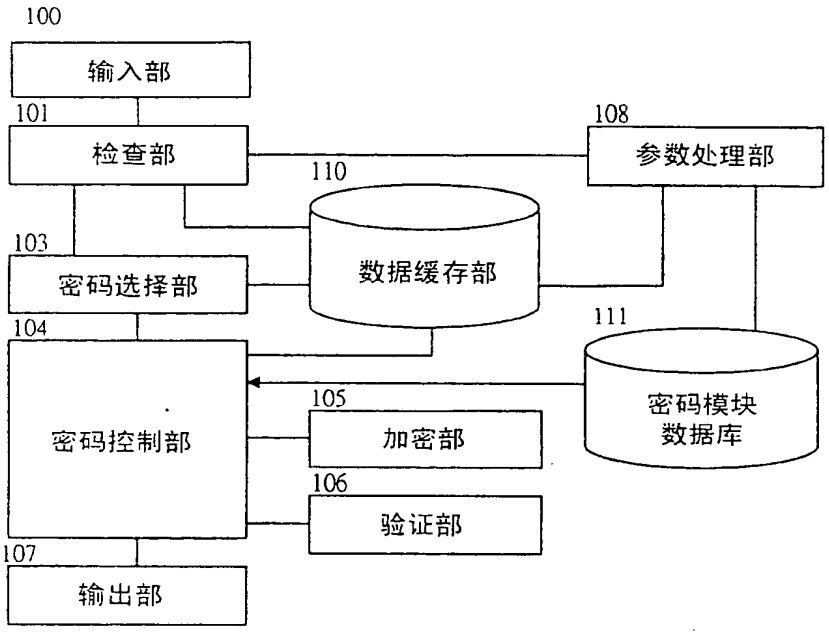

100
输入部
101
检查部
108
参数处理部
110
数据缓存部
103
密码选择部
111
密码模块
数据库
104
密码控制部
105
加密部
106
验证部
107
输出部

图 16

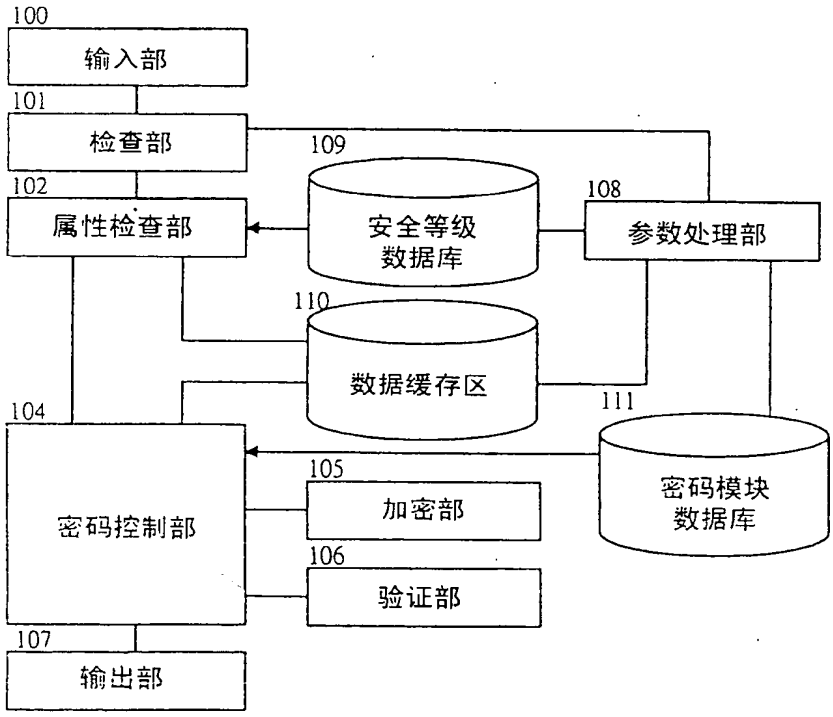

100
输入部
101
检查部
109
102
属性检查部
安全等级
数据库
108
参数处理部
110
数据缓存区
111
104
密码控制部
105
加密部
密码模块
数据库
106
验证部
107
输出部

图 17